Submission deadline– Long Term CFP

OPEN ACCESS

Call for Papers

Special Issue on

Security and Safety in Medical and Healthcare

Guest Editors:

➢ **Hairong Zheng**, Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, China
➢ **Jinglong Wu**, Okayama University, Japan
➢ **Huiyu Zhou**, University of Leicester, UK

Call for Papers

Special Issue on

Security and Safety in Medical and Healthcare

Background

With the widespread application of information and the booming development of cyberspace, the medical industry is experiencing an unprecedented digital transformation. On the one hand, the demand for medical data sharing is increasing and the World Health Organization has been continuously advocating and promoting data interoperability to consolidate the global health security barrier since 2022. However, data breaches occur, and medical data leakage or fake data fraud have occurred in the past 5 years, which highlights the urgency of medical data privacy protection and secure transmission. On the other hand, the application of artificial intelligence (AI) in medical imaging diagnosis and health management is expanding, but it also brings new security risks, such as model poisoning and adversarial attacks. The amount of data recorded in the medical industry is huge, far exceeding the industry average, and there is an urgent need for effective security solutions.

Aims and Scope of the Special Issue

Security and Safety (S&S) focuses on the intersection of cyber security and functional safety and launched this special issue on "**Security and Safety in Medical and Healthcare**", aiming to provide a platform for the global academic and industrial communities to discuss issues related to medical data sharing and security of-driven medical systems. This special issue will focus on key technologies such as privacy protection, secure transmission, risk assessment, and active defense, to promote the safe development of the medical.

This special issue covers (but not limited to) the following topics:

- Medical instrument data security collection and trusted storage technology for privacy protection
- Medical data trusted analysis methods and secure applications based on privacy computing
- Medical data clinical representation and anonymous sharing technology integrated with privacy enhancement
- Medical data secure transmission technology
- Privacy protection technology in medical data processing and analysis
- Security risk assessment in AI-driven medical systems
- Active technology in AI-driven medical systems
- Comprehensive security solution for medical data sharing and AI systems
- Medical data security decision-making and user behavior based on cognitive psychology

Submissions

Authors should submit their manuscripts online directly at: https://sands.nestor-edp.org and choose, during submission, the special issue: **Security and Safety in Medical and Healthcare**. All relevant papers will be carefully considered and peer-reviewed by a distinguished team of international experts. The instructions for authors are detailed at: https://sands.edpsciences.org/author-information/instructions-for-authors.

Submission deadline – Long Term Call for Papers

Article Processing Charges - S&S is an Open Access journal and no APCs in 2025.

Guest Editors

Hairong Zheng, Shenzhen Institutes of Advanced Technology,

Chinese Academy of Sciences, China, hr.zheng@siat.ac.cn

Jinglong Wu, Okayama University, Japan, wu@mech.okayama-u.ac.jp

Huiyu Zhou, University of Leicester, UK, hz143@leicester.ac.uk

Contact

Yuanyuan Liu, *Security and Safety* Editorial Office, sands@edpsciences.org

S&S Website